Fig. 1 PRIOR ART

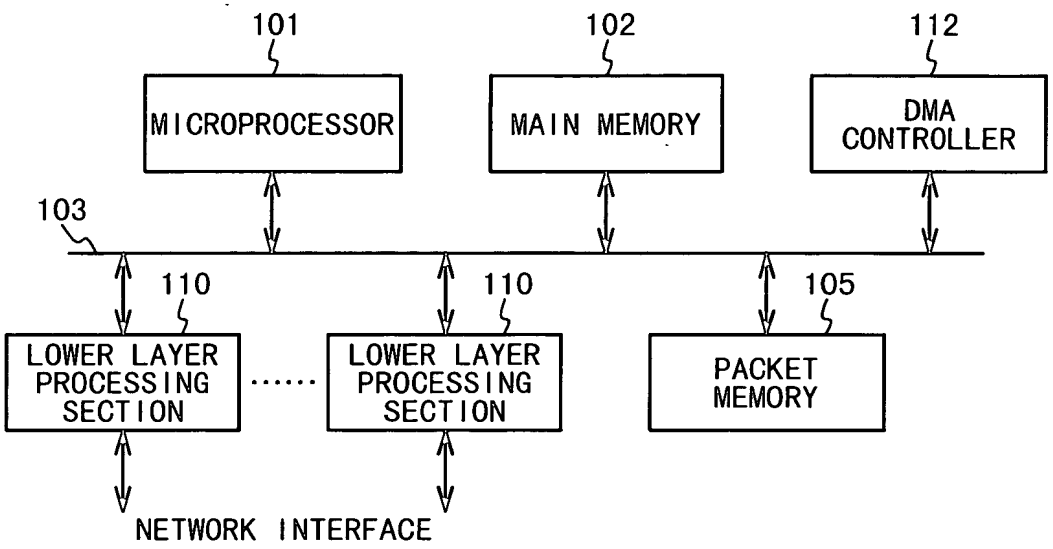


Fig. 2

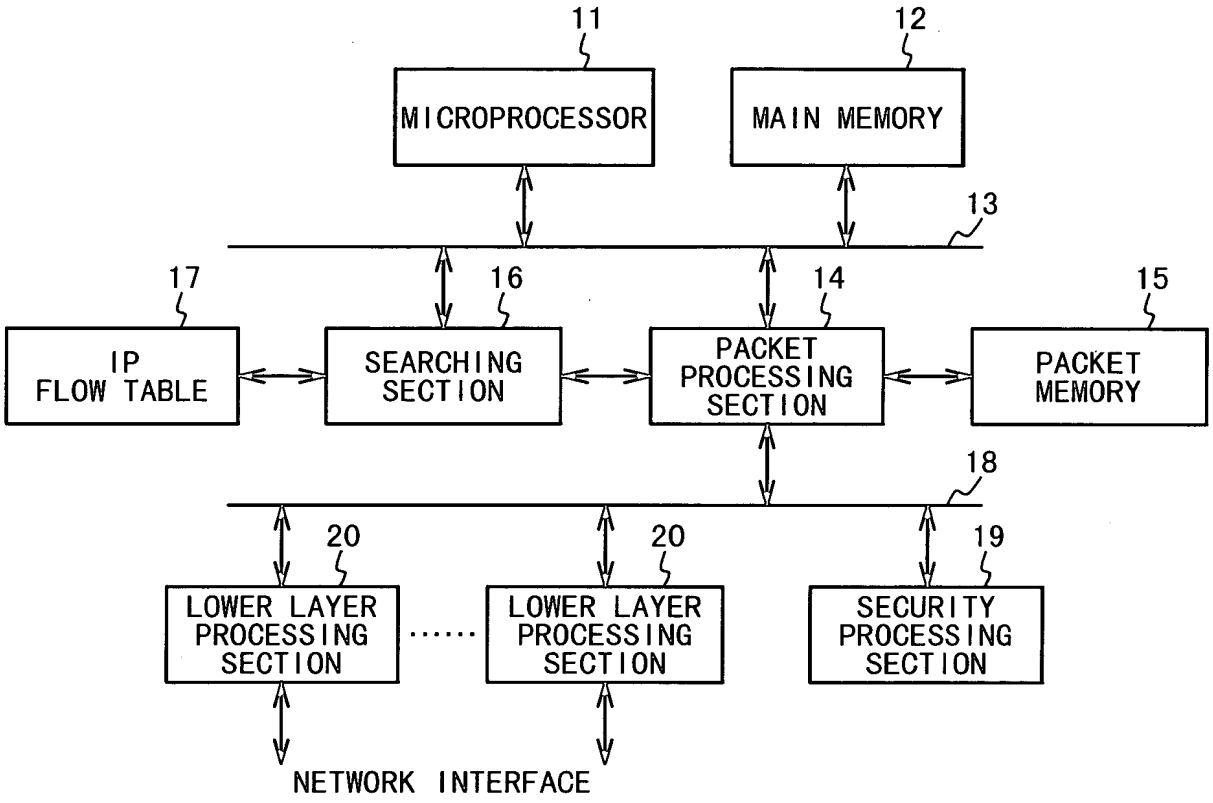

11
12
MICROPROCESSOR
MAIN MEMORY
13
17
16
14
15
IP
FLOW TABLE
SEARCHING
SECTION
PACKET
PROCESSING
SECTION
PACKET
MEMORY
18
20
20
19
LOWER LAYER
PROCESSING
SECTION
LOWER LAYER
PROCESSING
SECTION
SECURITY
PROCESSING
SECTION
NETWORK INTERFACE

Fig. 3

SEARCH KEY		ROUTING RESULT			SECURITY DATA			
IP SOURCE ADDRESS	IP DESTINATION ADDRESS	MAC SOURCE ADDRESS	MAC DESTINATION ADDRESS	OUTPUT PORT NO.	ENCRYPTION ALGORITHM	ENCRYPTION KEY	NEW IP SOURCE ADDRESS	NEW IP DESTINATION ADDRESS
AA BB CC DD	EE FF GG HH	123456	789012	2				
AA BB CC DD	KK LL MM NN			9	DES-CBC	XXXXXX	AA BB CC XX	KK LL MM YY
AA BB CC XX	KK LL MM YY	123456	789012	2				
KK LL MM YY	AA BB CC XX			9	DES-CBC	YYYYYY		
... ...	... ...	... ...	... ...	... ...	... ...	... ...	... ...	... ...

Fig. 4

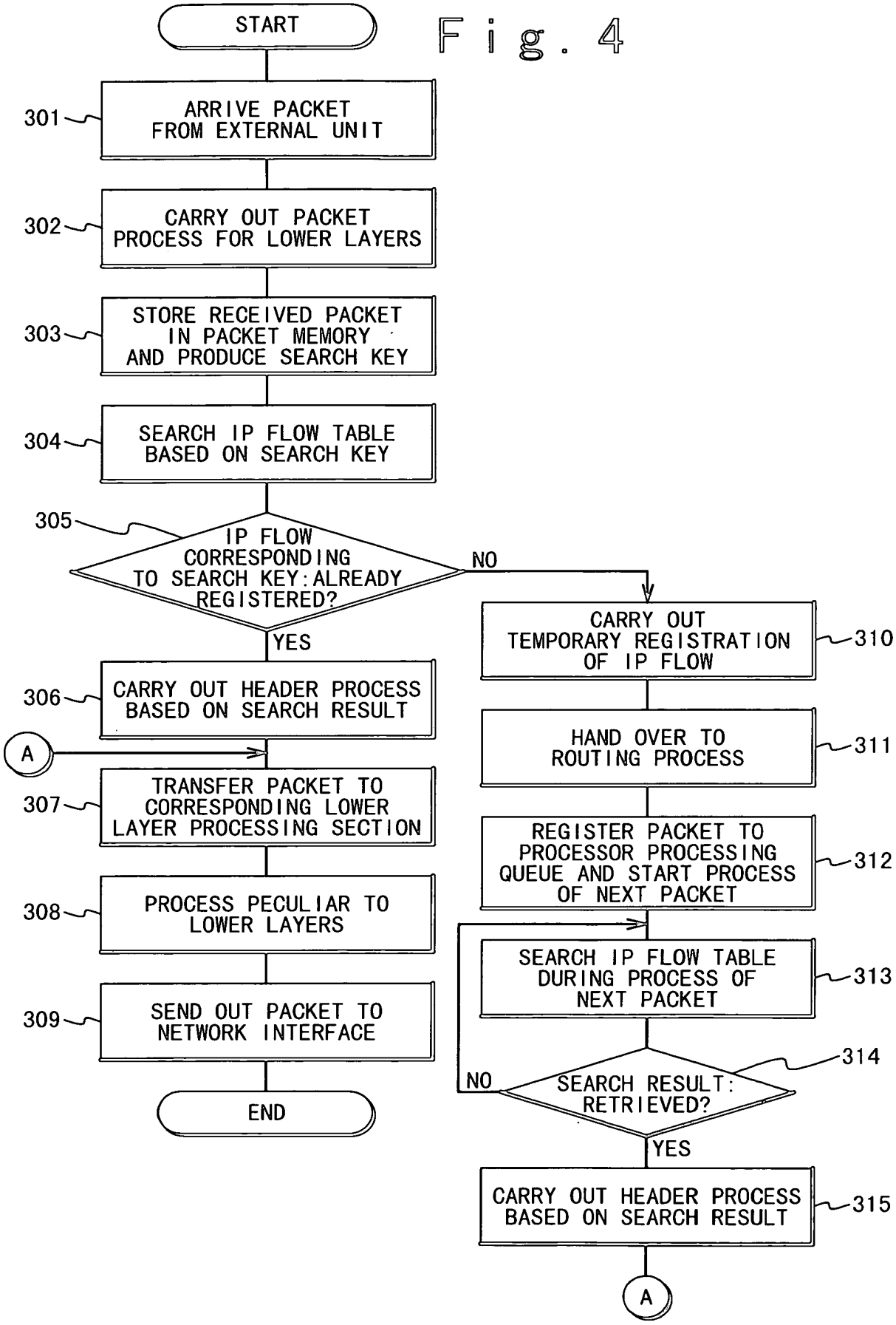

START
301
ARRIVE PACKET FROM EXTERNAL UNIT
302
CARRY OUT PACKET PROCESS FOR LOWER LAYERS
303
STORE RECEIVED PACKET IN PACKET MEMORY AND PRODUCE SEARCH KEY
304
SEARCH IP FLOW TABLE BASED ON SEARCH KEY
305
IP FLOW CORRESPONDING TO SEARCH KEY: ALREADY REGISTERED?
NO
YES
306
CARRY OUT HEADER PROCESS BASED ON SEARCH RESULT
A
307
TRANSFER PACKET TO CORRESPONDING LOWER LAYER PROCESSING SECTION
308
PROCESS PECULIAR TO LOWER LAYERS
309
SEND OUT PACKET TO NETWORK INTERFACE
END
310
CARRY OUT TEMPORARY REGISTRATION OF IP FLOW
311
HAND OVER TO ROUTING PROCESS
312
REGISTER PACKET TO PROCESSOR PROCESSING QUEUE AND START PROCESS OF NEXT PACKET
313
SEARCH IP FLOW TABLE DURING PROCESS OF NEXT PACKET
314
SEARCH RESULT: RETRIEVED?
NO
YES
315
CARRY OUT HEADER PROCESS BASED ON SEARCH RESULT
A

Fig. 5

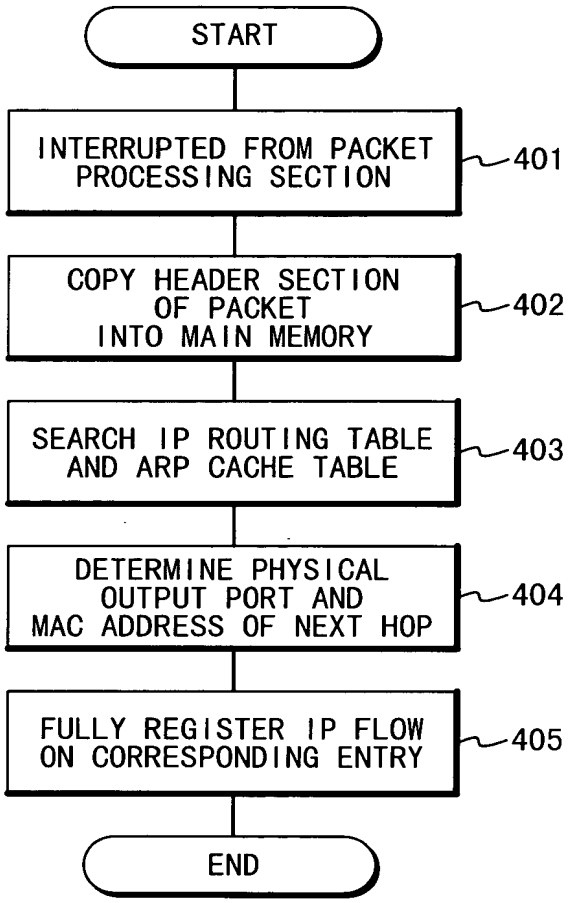

START
INTERRUPTED FROM PACKET PROCESSING SECTION
401
COPY HEADER SECTION OF PACKET INTO MAIN MEMORY
402
SEARCH IP ROUTING TABLE AND ARP CACHE TABLE
403
DETERMINE PHYSICAL OUTPUT PORT AND MAC ADDRESS OF NEXT HOP
404
FULLY REGISTER IP FLOW ON CORRESPONDING ENTRY
405
END

Fig. 6A

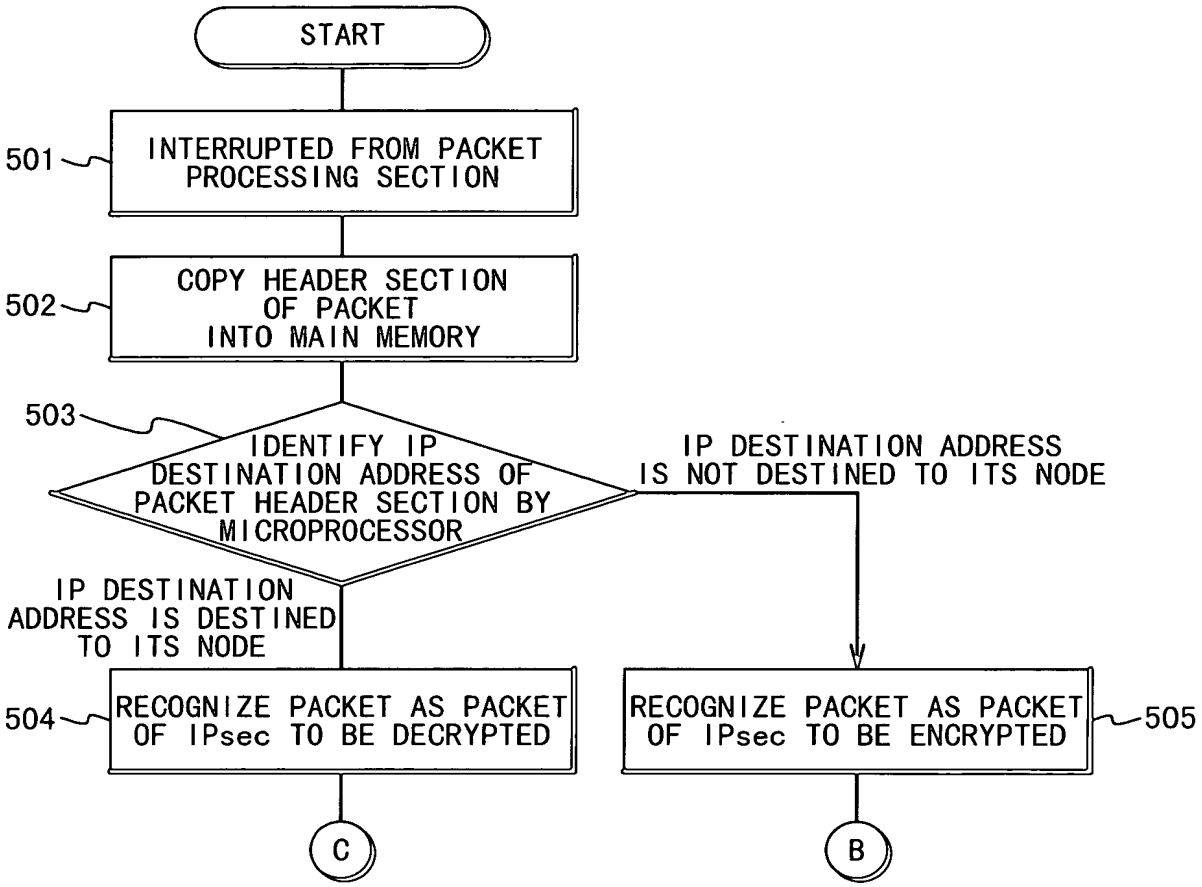

START
501
INTERRUPTED FROM PACKET PROCESSING SECTION
502
COPY HEADER SECTION OF PACKET INTO MAIN MEMORY
503
IDENTIFY IP DESTINATION ADDRESS OF PACKET HEADER SECTION BY MICROPROCESSOR
IP DESTINATION ADDRESS IS NOT DESTINED TO ITS NODE
IP DESTINATION ADDRESS IS DESTINED TO ITS NODE
504
RECOGNIZE PACKET AS PACKET OF IPsec TO BE DECRYPTED
RECOGNIZE PACKET AS PACKET OF IPsec TO BE ENCRYPTED
505
C
B

Fig. 6B

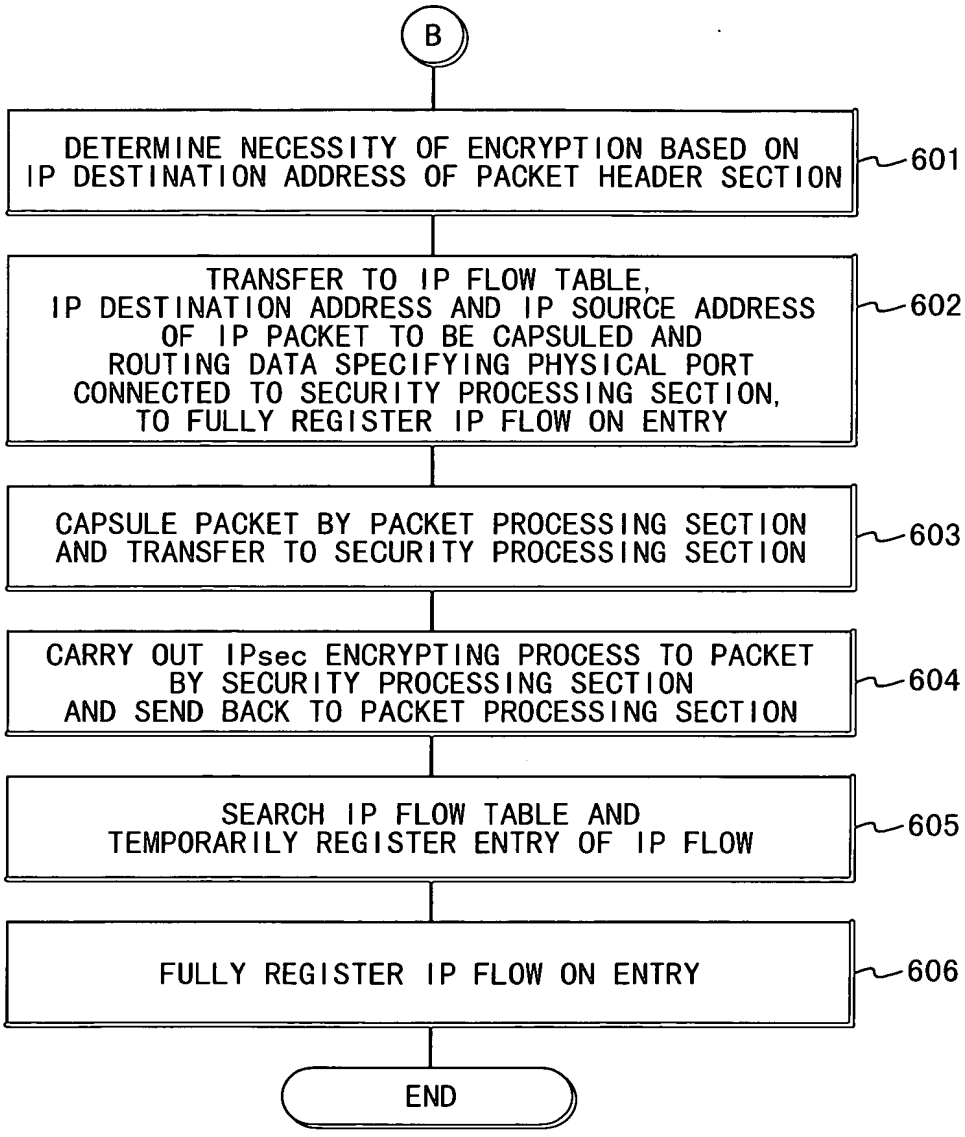

B
DETERMINE NECESSITY OF ENCRYPTION BASED ON IP DESTINATION ADDRESS OF PACKET HEADER SECTION
601
TRANSFER TO IP FLOW TABLE, IP DESTINATION ADDRESS AND IP SOURCE ADDRESS OF IP PACKET TO BE CAPSULED AND ROUTING DATA SPECIFYING PHYSICAL PORT CONNECTED TO SECURITY PROCESSING SECTION, TO FULLY REGISTER IP FLOW ON ENTRY
602
CAPSULE PACKET BY PACKET PROCESSING SECTION AND TRANSFER TO SECURITY PROCESSING SECTION
603
CARRY OUT IPsec ENCRYPTING PROCESS TO PACKET BY SECURITY PROCESSING SECTION AND SEND BACK TO PACKET PROCESSING SECTION
604
SEARCH IP FLOW TABLE AND TEMPORARILY REGISTER ENTRY OF IP FLOW
605
FULLY REGISTER IP FLOW ON ENTRY
606
END

Fig. 6C

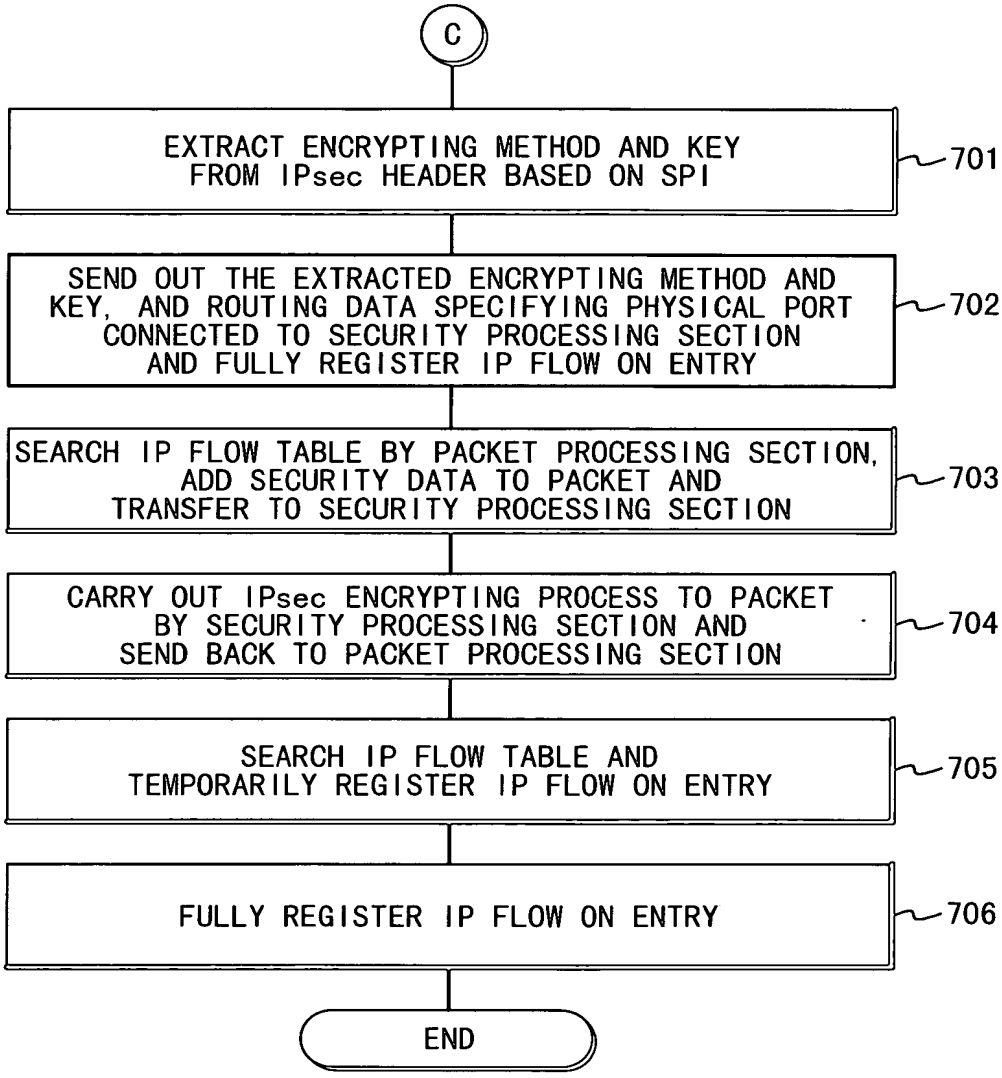
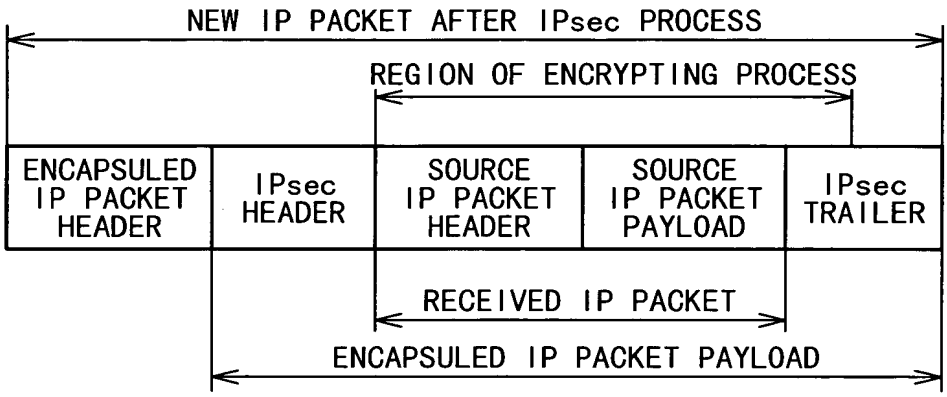

C
EXTRACT ENCRYPTING METHOD AND KEY FROM IPsec HEADER BASED ON SPI
701
SEND OUT THE EXTRACTED ENCRYPTING METHOD AND KEY, AND ROUTING DATA SPECIFYING PHYSICAL PORT CONNECTED TO SECURITY PROCESSING SECTION AND FULLY REGISTER IP FLOW ON ENTRY
702
SEARCH IP FLOW TABLE BY PACKET PROCESSING SECTION, ADD SECURITY DATA TO PACKET AND TRANSFER TO SECURITY PROCESSING SECTION
703
CARRY OUT IPsec ENCRYPTING PROCESS TO PACKET BY SECURITY PROCESSING SECTION AND SEND BACK TO PACKET PROCESSING SECTION
704
SEARCH IP FLOW TABLE AND TEMPORARILY REGISTER IP FLOW ON ENTRY
705
FULLY REGISTER IP FLOW ON ENTRY
706
END

Fig. 7


NEW IP PACKET AFTER IPsec PROCESS
REGION OF ENCRYPTING PROCESS
ENCAPSULED IP PACKET HEADER
IPsec HEADER
SOURCE IP PACKET HEADER
SOURCE IP PACKET PAYLOAD
IPsec TRAILER
RECEIVED IP PACKET
ENCAPSULED IP PACKET PAYLOAD